

Exhibit A

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK**

CORPORATE RISK HOLDINGS, LLC, solely in its
capacity as the PLAN ADMINISTRATOR UNDER
THE AMENDED JOINT CHAPTER 11 PLAN OF
ALTEGRITY, INC., ET AL.,

Plaintiff,

-against-

SHARON T. ROWLANDS,

Defendant.

Index No.

SUMMONS

Plaintiff designates New York
County as the place of trial

To the above-named Defendant: Sharon T. Rowlands - 270 Broadway APT 21A
New York, NY 10007-2345


You are hereby summoned to answer the complaint in this action, and to serve a copy of your answer on the Plaintiff's attorneys within twenty (20) days after the service of this summons, exclusive of the day of service, where service is made by delivery upon you personally within the State, or within thirty (30) days after completion of service where service is made in any other manner. In case of your failure to answer, judgment will be taken against you by default for the relief demanded in the complaint.

Plaintiff designates New York County as the place of trial.

Plaintiff hereby demands a trial by jury.

Dated: May 26, 2017
New York, New York

BERNSTEIN LIEBHARD LLP

By: 
Stanley D. Bernstein
Stephanie M. Beige
Laurence J. Hasson
10 East 40th Street
New York, NY 10016
Telephone: 212-779-1414
Facsimile: 212-779-3218

Attorneys for Plaintiff

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK**

CORPORATE RISK HOLDINGS, LLC, solely in
its capacity as the PLAN ADMINISTRATOR
UNDER THE AMENDED JOINT CHAPTER 11
PLAN OF ALTEGRITY, INC., ET AL.,

Plaintiff,

-against-

SHARON T. ROWLANDS,

Defendant.

Index No. _____

**COMPLAINT AND
DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

	<u>Page</u>
I. NATURE OF THE ACTION	2
A. Plaintiff, the Plan Administrator, for the Benefit of the Creditors Represented by the Committee, Seeks Damages Sustained by USIS from Former Director Defendant Rowlands for Having Consciously Disregarded Her Duties as a Director	2
B. Defendant Rowlands Consciously Disregarded Her Duty to Oversee and Monitor USIS's Cybersecurity Practices in Light of the Known Risk	3
C. The Data Breach and USIS's Failure to Protect the Confidential Data	6
D. Investigations Conducted after the Data Breach Expose USIS's Substandard Cybersecurity Measures	7
II. JURISDICTION AND VENUE	11
III. THE PARTIES	11
IV. SUBSTANTIVE ALLEGATIONS	13
A. Background	13
B. Protecting the Confidential Data was Critical to USIS's Relationship with OPM	15
C. USIS Improperly Focused on OPM's Minimum Security Compliance Criteria Rather Than on the Known Risk the Company was Facing	16
D. The Data Breach - USIS's Substandard Cybersecurity Defenses Leaves the Company Vulnerable to a Cyberattack	17
E. USIS's Remediation Efforts Reveal the Fundamental Flaws in USIS's Cybersecurity	20
F. USIS is Forced to Shutter Its Business and USIS and Altegrity File for Bankruptcy	21
G. USIS is Subjected to Congressional Scrutiny	24
H. Defendant Rowlands and the Board Had a Duty to Oversee and Monitor USIS's Response to Known Cybersecurity Risks	25
1) The OPM Contracts Were Material to USIS's Operations	26

2)	Safeguarding the Confidential Data Was Critical to USIS's Relationship with OPM and to National Security.....	27
3)	The Nature of USIS's Business Made it Target for an APT Attack	27
4)	Defendant Rowlands Knew USIS Suffered from Weak Internal Controls	31
I.	In the Face of the Known Risks, Defendant Rowlands and the Board Consciously Failed to Monitor and Oversee USIS's Cybersecurity Practices	34
FIRST CAUSE OF ACTION Against Defendant Rowlands for Breach of Fiduciary Duty.....		36
PRAYER FOR RELIEF		37
JURY TRIAL DEMANDED		37

Corporate Risk Holdings, LLC, solely in its capacity as the Plan Administrator (“Plaintiff”) appointed under the Amended Joint Chapter 11 Plan of Altegrity, Inc., *et al.* (the “Plan”),¹ brings this action on behalf of US Investigations Services, LLC (“USIS” or the “Company”) at the direction of the Specified Claims Oversight Committee (the “Committee”) by and through its undersigned counsel to recover the damages sustained by USIS, a subsidiary of Altegrity, Inc. (“Altegrity”), as a result of Defendant Sharon T. Rowlands’ breaches of her fiduciary duties as a member of the Board of Directors of USIS (the “Board”).²

Plaintiff alleges the following upon information and belief. This information and belief is based upon, among other things, counsel’s investigation into the 2013-2014 data breach of USIS, including, without limitation: (a) a review and analysis of confidential internal documents of USIS; (b) a review and analysis of press releases, public statements, news articles, and other publicly available information, including transcripts and filings made available by government agencies and the U.S. House Committee on Oversight and Government Reform (the “House Oversight Committee”); (c) a review and analysis of other complaints filed against USIS; and (d) other publicly available information, including the United States National Institute of

¹ *In re: Altegrity, Inc., et al.*, Case No. 15-10226 (LSS), shall be referred to herein as the “Bankruptcy.” Capitalized terms used but not defined herein shall have the meanings ascribed to them in the Plan confirmed by the United States Bankruptcy Court for the District of Delaware on August 14, 2015.

² Plaintiff brings this action solely in its capacity as the Plan Administrator, pursuant to the Plan, at the direction of the Committee, which is the real party in interest, and solely for the benefit of the creditors of the Liquidating Debtors. Accordingly, the allegations herein are based upon the investigation of the Committee and its undersigned counsel and therefore, the Plaintiff has not made any independent evaluation of the claims set forth herein. In addition, Plaintiff brings this action without prejudice to Corporate Risk Holdings, LLC’s ability, as Plan Administrator or otherwise, to take any position with respect to litigation, or proofs of claim asserted in the Bankruptcy, against it or its affiliates concerning the matters set forth herein.

Standards Technology (“NIST”) “Information Security: Recommended Security Controls for Federal Information Systems and Organizations.”

Pursuant to the Plan, the claims set forth herein that belonged to USIS prior to the Bankruptcy, now vest with the Reorganized Debtor and are to be exercised by the Plaintiff at the direction of the Committee and for the benefit of the creditors the Committee represents.

I. NATURE OF THE ACTION

A. Plaintiff, the Plan Administrator, for the Benefit of the Creditors Represented by the Committee, Seeks Damages Sustained by USIS from Former Director Defendant Rowlands for Having Consciously Disregarded Her Duties as a Director

1. Plaintiff brings this action to recover damages sustained by USIS as a result of Defendant Rowlands’ breaches of her fiduciary duties as a Board member to oversee and monitor USIS’s cybersecurity practices in response to the known risk of a cyberattack.³

2. As a result of Defendant Rowlands’ and the Board’s complete abdication of their responsibilities, USIS’s woefully deficient cybersecurity practices went unaddressed, leaving the Company virtually defenseless against a crippling and *preventable* cyberattack in 2013-2014 (the “Data Breach”) that destroyed USIS’s business; forced USIS and its parent company, Altegrity, into bankruptcy; and compromised national security by exposing the sensitive and confidential background information of over 33,000 actual and potential employees of the U.S. government (the “Confidential Data”) to malicious state-sponsored actors.

3. Defendant Rowlands’ failure to oversee and monitor USIS’s cybersecurity practices was a conscious disregard for her responsibilities as a director, amounting to bad faith.

³ Pursuant to the Plan, Defendant Rowlands is the only member of the Board that can be named as a defendant in this action.

At all relevant times leading up to the Data Breach, Defendant Rowlands and the Board knew that the risk of a cyberattack at USIS was a genuine risk that would have devastating effects on the Company. Specifically, Defendant Rowlands and the Board knew: (1) that USIS was a target for a cyberattack due to the nature of its business and the type of Confidential Data maintained on its network; (2) that the risk of a cyberattack at USIS was increasing; (3) that the consequences of a cyberattack would be devastating to the Company and would compromise national security; and (4) that USIS suffered from weak internal controls, warranting closer monitoring of such risks by the Board.

4. Nevertheless, Defendant Rowlands and the Board willfully ignored the increasing risk of a cyberattack at USIS and made no effort to address or prevent the disaster that would ensue as a result of an attack.

B. Defendant Rowlands Consciously Disregarded Her Duty to Oversee and Monitor USIS's Cybersecurity Practices in Light of the Known Risk

5. Defendant Rowlands and the Board were well aware of the risk of a cyberattack at USIS and the importance of taking adequate precautions to prevent an attack. In March 2012 (prior to the Data Breach), Defendant Rowlands herself publicly warned that “cybersecurity” was one of “the most significant issues for business today” and emphasized that companies handling confidential information like USIS had to be proactive with respect to preventing cyberattacks, and had to have procedures in place to “constantly” test their cybersecurity systems and procedures.

6. Defendant Rowlands and the Board knew that USIS was a likely target for a cyberattack and that the risk of such an attack was increasing. The sensitive nature of the Confidential Data that USIS collected made it appealing to malicious actors who could use it to compromise U.S. missions. In the years leading up to the Data Breach, there was a dramatic

increase in nation-state directed cyberattacks aimed at stealing confidential and sensitive data from government agencies and contractors, such as USIS. In particular, there were myriad warnings about the growing threat of Advanced Persistent Threat (“APT”) attacks – the exact type of attack that was used in the Data Breach.

7. Defendant Rowlands and the Board further knew that a cyberattack at USIS was an enterprise-wide risk that would be devastating for the Company and would jeopardize national security. Unlike frequent data breaches seeking credit card information from retail vendors which can be remedied by simply providing credit monitoring to potential victims and paying modest damages to affected card users, a data breach at USIS would not only expose government employees’ and applicants’ personal and potentially damaging investigation information, but it would also jeopardize national security by enabling enemies of the United States to identify federal employees (including federal agents working overseas) and exploit the confidential information for their benefit.

8. Defendant Rowlands and the Board knew that the ramifications of a data breach at USIS would jeopardize USIS’s business relationships with the U.S. Office of Personnel Management (“OPM”) and other federal agencies – USIS’s most significant revenue source. Indeed, USIS garnered most, if not all, of its business from OPM and other government agencies. These contracts were highly lucrative and material to both USIS and Altegrity. Defendant Rowlands and the Board knew that a failure on the part of USIS to adequately protect the Confidential Data entrusted to it by OPM would threaten the Company’s ongoing relationship with OPM and jeopardize USIS’s entire operation.

9. Lastly, Defendant Rowlands and the Board knew that USIS suffered from weak internal controls that necessitated the Board’s careful oversight and monitoring of the

Company's response to the risk of a cyberattack. Specifically, Defendant Rowlands and the Board: (1) knew that USIS senior management had a history of taking shortcuts with respect to the Company's work for OPM; (2) knew that USIS senior management had engaged in fraudulent billing practices in order to increase revenues and earn bonuses; (3) knew that USIS senior management compromised national security by fraudulently reporting that incomplete background investigations for OPM were complete; and (4) knew that Congress and various government agencies were questioning the quality and integrity of USIS's background investigation work, including the Company's background investigations of former intelligence contractor Edward Snowden and former defense contractor Aaron Alexis.

10. USIS's weak internal controls, as well as the Company's history of cutting corners to increase revenues, should have raised a red flag to Defendant Rowlands and the Board that USIS required careful oversight and monitoring and should not be left to its own devices with respect to its response (if any) to the known enterprise-wide risk USIS was facing.

11. Nevertheless, internal USIS documents show that Defendant Rowlands and the Board failed to exercise *any* oversight over USIS's cybersecurity practices, and thus completely disabled themselves from being informed as to how vulnerable USIS was to a likely attack.

12. For example, based on internal Board minutes from Board meetings held from February 12, 2012 (over a year prior to the Data Breach) through March 31, 2014 (the "Board Minutes"), the Board did not discuss USIS's cybersecurity measures or the increasing risk of an attack. For example, the Board Minutes reflect that the Board was not briefed on USIS's cybersecurity practices, the Board did not question USIS executives as to whether the Company's cybersecurity measures were adequate in light of the known risk of a cyberattack, and the Board did not discuss what steps, if any, USIS was taking any steps to thwart a likely

attack. In fact, according to the Board Minutes, USIS's cybersecurity policies and procedures were not a topic of discussion at any of the Board meetings leading up to the Data Breach. As a consequence, Defendant Rowlands and the Board were completely in the dark as to what steps, if any, USIS was taking to protect the Company from the increasing risk of a cyberattack.

13. Had Defendant Rowlands and the Board satisfied their obligations as directors to oversee and monitor USIS's cybersecurity measures in light of the known risk of a cyberattack, the deficiencies in USIS's cybersecurity practices would have been exposed and could have been addressed before the Confidential Data was compromised.

C. The Data Breach and USIS's Failure to Protect the Confidential Data

14. On April 19, 2013, unknown to USIS, malicious actors breached USIS's systems by exploiting a "Top Ten" security vulnerability in USIS's Internet-facing systems – specifically, the Company's Systems Applications Products ("SAP") system.

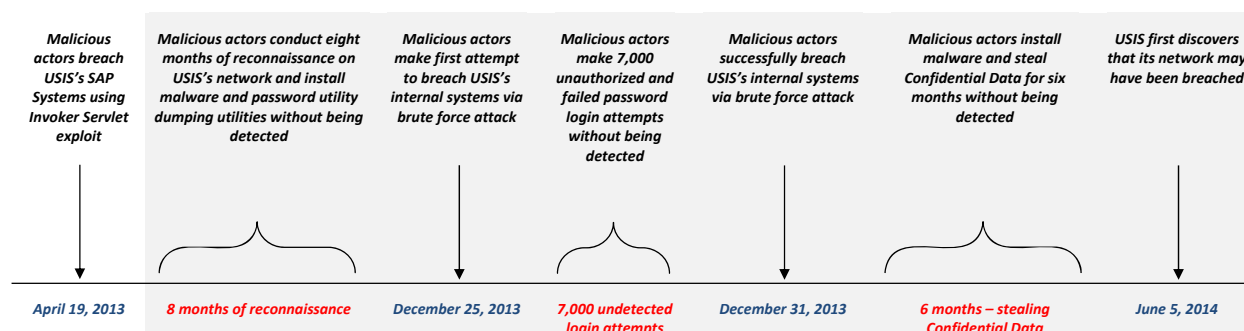
15. After performing approximately *eight months* of reconnaissance on USIS's network undetected (due to USIS's inadequate intrusion detection systems and controls), the malicious actors exploited a second vulnerability: *USIS's failure to properly segment and isolate its internal systems containing Confidential Data from its Internet-facing SAP Systems.*⁴ USIS's failure to properly segment its systems gave the malicious actors access to the Confidential Data stored on USIS's internal systems.

⁴ Network segmentation is the division of a network into subnetworks with varying degrees of security to restrict access to sensitive data by adding layers of security to those systems containing sensitive data.

16. On December 25, 2013, the malicious actors commenced a “brute force” attack that went undetected by USIS and allowed them to break into USIS’s internal systems less than one week later, on December 31, 2013.⁵

17. Upon breaking into USIS’s internal systems, the malicious actors began collecting the Confidential Data on the Company’s network. Due to USIS’s lack of basic intrusion detection measures, the malicious actors continued this activity for approximately *six months without being detected*.

18. USIS first detected the malicious actors on June 5, 2014 (*over a year after the initial breach*). By then, however, the Confidential Data of over 33,000 federal employees, potential employees, and contractors had been compromised. A timeline of the attack is set forth below:



D. Investigations Conducted after the Data Breach Expose USIS’s Substandard Cybersecurity Measures

19. Investigations conducted after the Data Breach by both USIS and OPM revealed the extent to which USIS’s cybersecurity deficiencies left the Company virtually defenseless against the Data Breach. Despite the dramatic increase in nation-state directed cyberattacks

⁵ A “brute force” attack is a common and easily detectable hacking technique to guess a password through trial and error as opposed to logic.

aimed at stealing confidential and sensitive data from government contractors, and the myriad warnings about the growing threat of an APT attack, USIS failed to implement basic and available network defenses to address USIS's security risk. As described herein, USIS failed to have even the most basic cybersecurity measures in place.

20. **First**, USIS failed to properly segment and isolate its internal systems containing Confidential Data from its Internet-facing systems which gave the malicious actors easy access to the Confidential Data. Although network segmentation is a standard security measure, USIS failed to properly implement this basic security measure to protect the Confidential Data.

21. **Second**, USIS failed to fix the widely-known "**Top Ten**" security vulnerability in its Internet-facing SAP systems, known as the "Invoker Servlet," despite the availability of a patch as early as December 2010. USIS's failure to follow routine patch management practices and fix the known vulnerability in its SAP systems afforded the malicious actors easy access to the Confidential Data.

22. **Third**, USIS's inadequate intrusion detection systems, controls and IT staffing, allowed the malicious actors to perform approximately **eight months** of reconnaissance on USIS's network **undetected**.

23. **Fourth**, USIS lacked the basic security defenses to thwart a brute force attack, including standard intrusion detection and password protection mechanisms that are present on virtually every secure network which limit the number of attempted logins before a user is locked out of a system. This fundamental security failure allowed the malicious actors to enter **7,000 unauthorized login attempts over a period of three days** without being locked out of, or otherwise hindered from trying to break into USIS's internal systems, ultimately gaining access to USIS's internal network **without detection**.

24. These failed login attempts should have been recorded in USIS's security logs, and should have alerted the Company to the brute force attack in progress. Moreover, USIS failed to ensure that the Company had adequate cybersecurity controls and staffing such that ***no one at the Company routinely reviewed the security logs***. Accordingly, the brute force attack, which potentially could have been detected (and could have prompted USIS to sever its internal systems before any compromise of Confidential Data), went completely unnoticed.

25. Compounding these, and other, fundamental security flaws was USIS's shocking failure to have adequate and qualified IT personnel in charge of the Company's cybersecurity. Specifically, despite the sensitive nature of the Confidential Data USIS was protecting, the Company only had approximately ***eight*** IT employees to handle all of the switches, routers, firewalls and servers for the entire Company.

26. As a consequence, USIS lacked sufficient controls and failed to properly monitor its network for malicious traffic or activity. In fact, USIS provided only limited network monitoring coverage from ***Monday through Friday, from 7:00 a.m. to 4:00 p.m., with no weekend support. After 4:00 p.m., nobody was watching USIS's network.*** Twenty-four hour network monitoring was critical for USIS in light of the Confidential Data on its network and the known and increasing risk of an attack.

27. USIS's security deficiencies were basic cybersecurity measures that should have been addressed long before the Data Breach. Had these deficiencies been remedied, the Data Breach likely could have been prevented, and most definitely could have been mitigated.

28. USIS's cybersecurity measures were so deficient, that The U.S. Department of Homeland Security's Computer Emergency Readiness Team ("US-CERT") issued a devastating report after the Data Breach, concluding that USIS's network ***required a complete overhaul***:

[t]he network environment at USIS is lacking proper network segmentation such that it is impossible to differentiate the network traffic for our analysis from the traffic that is beyond the scope of assessment. While USIS identified that the scope would only include two of their subnets, we observed over 400 subnets traversing the core network during the hunt analysis. Based on the traffic we are seeing, US-CERT was unable to accurately vet all ingress and egress points. Our recommendation is for a complete rebuild and careful copying over of data, and this is likely to take months to do correctly. Existing systems must be considered vulnerable unless they are disconnected or the data is deleted. In addition, we cannot state at this time with full confidence that the intruder has been removed. In order to reach a level of comfort and assurance in the network at USIS, a defense-in-depth security approach is recommended. (emphasis added).

29. Based on US-CERT's report, OPM concluded that *USIS's network was not reasonably secure, and that the network needed to be completely rebuilt before USIS would be allowed to perform further work for the agency.*

30. As a result, USIS lost all of its federal background investigation business, as OPM and other agencies terminated their contracts with the Company. Given the materiality of this business to USIS (and Altegrity), USIS was forced to wind down its business operations and USIS and its parent company Altegrity were forced to file for bankruptcy.

31. Had Defendant Rowlands and the Board satisfied their obligations as directors to oversee and monitor USIS's cybersecurity practices in light of the growing risk of a cyberattack, USIS's woefully deficient cybersecurity issues would have been exposed and could have been addressed.

32. As a result of Defendant Rowlands' breaches of her fiduciaries duties, USIS has been significantly damaged, in that USIS: (1) suffered the devastating (and preventable) Data Breach that resulted in the exfiltration of the Confidential Data of tens of thousands of federal employees and applicants seeking sensitive national security clearances; (2) received Stop-Work Orders from OPM; (3) was forced to terminate its workforce and spend millions of dollars to remediate its network; (4) lost its lucrative contracts with OPM and other federal agencies;

(5) ceased to exist as a going concern; and (6) was exposed to litigation from federal agencies and federal employees for compromising the Confidential Data. Defendant Rowlands' breaches of her fiduciary duties also caused USIS and its parent company Altegrity to file for Chapter 11 bankruptcy and threatened the wholesale degradation of national security.

II. JURISDICTION AND VENUE

33. This Court has jurisdiction pursuant to CPLR §§ 301 and 302, and venue is proper pursuant to CPLR § 503.

III. THE PARTIES

34. Plaintiff, solely in its capacity as the Plan Administrator under the Plan, is Corporate Risk Holdings, LLC (formerly known as Altegrity) with its corporate headquarters located at 600 Third Avenue, 4th Floor, New York, New York 10016.

35. The Plan Administrator was established under the Plan, as confirmed by the United States Bankruptcy Court for the District of Delaware by Order dated August 14, 2015. Pursuant to Sections 5.16(b) and 8.14 of the Plan, all of the Liquidating Debtors' rights to the Specified Litigation Claims are to be exercised by the Plan Administrator for, and at the direction of, the Committee, including the claims asserted against Defendant Rowlands in this action.⁶

36. The Committee was formed pursuant to Section 5.20 of the Plan and holds the rights to direct the Specified Litigation Claims on behalf of and for the benefit of the creditors the Committee represents.

⁶ Pursuant to ¶189 of Section 1.1 of the Plan, the Specified Litigation Claims includes, among other claims, "all claims or causes of action of a Liquidating Debtor against any of the Specified D&O Litigation Parties related to the actions or omissions of such parties. . . ."

37. Upon information and belief, Defendant Sharon T. Rowlands is a resident of New York, New York.

38. At all relevant times, Defendant Rowlands was a member of the Board of Directors of USIS. Defendant Rowlands was also a member of the Boards of Directors of Altegrity Holding, Corp., Altegrity Acquisition Corp., and Altegrity, as well as the Chief Executive Officer of Altegrity, with her principal place of business located at 600 Third Avenue, 4th Floor, New York, New York.

39. Upon information and belief, all relevant meetings of the Joint Board of Directors took place in New York, New York.

Relevant Non-Parties

40. Altegrity Holding Corp. was the holding company of Altegrity Acquisition Corp. and Altegrity.

41. Altegrity was a Delaware corporation with its corporate headquarters located at 600 Third Avenue, 4th Floor, New York, New York, and is now known as Corporate Risk Holdings, LLC.

42. USIS is a Delaware limited liability company with its headquarters in Falls Church, Virginia.

IV. SUBSTANTIVE ALLEGATIONS

A. Background

43. Prior to filing for Chapter 11 bankruptcy, Altegrity was a privately held global, diversified risk and information services company serving both commercial and government entities. Altegrity operated through three business segments: USIS, Kroll,⁷ and HireRight.⁸

44. USIS, which was the business segment that generated the most revenue for Altegrity, was a provider of background investigations and information management and security services to federal agencies. USIS was originally formed in 1996 from the privatization of a unit of OPM under the initiative of Congress to conduct background investigative services for OPM.

45. OPM is responsible for performing background investigations of current or prospective federal employees or contractors for over one hundred government agencies, including the Department of Justice, Department of Homeland Security, Department of Health and Human Services, Department of Transportation, Department of Treasury, and Department of Defense, Defense Intelligence Agency.

46. On average, OPM conducts over two million background investigations per year, and oversees 90% of all security clearance background investigations for the U.S. government. While OPM staff performs some of this work, given the high volume, OPM has historically outsourced most of the work to a small number of private companies, including USIS.

47. OPM's first contract with USIS was dated April 12, 1996. Under the terms of the contract, USIS began performing background investigations to provide a basis for determining

⁷ Kroll is a provider of investigative and due diligence advisory services, e-discovery technologies, data recovery solutions, and risk mitigation and verification services.

⁸ HireRight is a provider of employment background screening, drug/health screening, and employment eligibility solutions

(1) an individual's suitability for federal employment, and (2) whether an individual should be granted clearance for access to national security information. OPM continued to contract with USIS to perform background investigation work thereafter, and USIS's business expanded to perform other services for OPM and other federal agencies.

48. USIS operated through two business divisions: the Global Security & Solutions Division ("GS&S") and the Investigations Services Division ("ISD"). GS&S provided personnel information and security services, as well as litigation support, records management, and analytics primarily to federal agencies through its Background Investigation Support Services Contract with OPM (the "Support Contract"). This five-year Support Contract was awarded to USIS in 2011 and was valued at approximately \$288 million.

49. ISD was the largest commercial provider of background investigation services to the federal government due to its Background Investigation Fieldwork Contract with OPM (the "Fieldwork Contract"). This five-year Fieldwork Contract was likewise awarded to USIS in 2011, and was valued at approximately \$2.46 billion, making it the largest contract held by USIS, and a major revenue driver for both USIS and Altegrity.

50. Pursuant to the Fieldwork Contract, USIS was responsible for conducting the investigatory fieldwork on individuals seeking new or continued employment with federal agencies or one of their contractors. USIS was not responsible for determining whether an applicant received or retained security clearance (known as "adjudication"), but rather, was responsible for collecting and reporting key information that formed the basis of a federal agency's adjudication decision.

51. Depending upon the type of investigation at issue, USIS's fieldwork might entail conducting interviews of the applicant and/or friends or family of the applicant, conducting

educational or employment record checks, running law checks, and/or running a check of the applicant's credit history. The information USIS collected included extremely personal and potentially damaging information about the applicant, such as whether the applicant engaged in extramarital affairs, engaged in past drug use, had gambling problems, required psychological treatment or counseling, etc. Because the Confidential Data could be used to identify and exploit federal employees and compromise U.S. missions, it was a treasure chest for malicious actors and other enemies of the state.

52. Prior to the Data Breach, USIS employed over 5,700 individuals and generated approximately \$537.3 million in revenue for the twelve months ended June 30, 2014. USIS's revenue accounted for 39% of Altegrity's consolidated revenues during the same timeframe, whereas Kroll and HireRight accounted for 37% and 24%, respectively.

B. Protecting the Confidential Data was Critical to USIS's Relationship with OPM

53. The background investigations USIS conducted played a critical role in protecting national security. In a statement made to the House Oversight Committee on February 11, 2014, former OPM Director Katherine Archuleta expanded on the importance of USIS's background investigations and the Confidential Data, noting that it enabled federal agencies to make "an informed decision about security clearances" and:

support[s] a host of other determinations or adjudications, including eligibility for national security sensitive positions and logical or physical access to federal information, systems and facilities; suitability for Federal employment in the competitive service (pursuant to a suitability program that OPM itself administers); fitness requirements for excepted service positions; military accessions; and fitness requirements imposed on individuals working under Government contracts.

54. Accordingly, safeguarding the Confidential Data was paramount to USIS's continued relationship with OPM and was mandated by the Company's Fieldwork and Support Contracts (and by other federal security requirements).

55. While the Fieldwork and Support Contracts contained a minimum set of security criteria that USIS had to satisfy to obtain an "Authorization to Operate" ("ATO") from OPM, USIS had to go well beyond complying with those minimum requirements to actually safeguard the Confidential Data maintained on the Company's network. Broadly speaking, USIS had to assess and address its specific level of security risk.

56. For example, the Federal Information Security Management Act of 2002 ("FISMA"), 44 U.S.C. § 3541 et seq., stresses that federal agencies, and the entities that support those agencies (such as USIS), employ a "risk-based policy" to develop, document, and implement programs to provide information security for the data and systems that support the operations and assets of federal agencies.

57. NIST, which develops "information security standards and guidelines, including minimum requirements for federal information systems," stresses the importance of holding leaders and managers of organizations like USIS accountable for failing to appreciate and address the information security risks posed to their respective organizations.

58. Accordingly, in order to adequately secure the Confidential Data and maintain USIS's business relationship with OPM, USIS was required to understand and manage the specific cybersecurity risks the Company faced.

C. USIS Improperly Focused on OPM's Minimum Security Compliance Criteria Rather Than on the Known Risk the Company was Facing

59. Despite the need to take a risk-based approach to network security, USIS instead cut corners and focused solely on satisfying the minimum security compliance criteria. Thus,

while USIS obtained Authorizations to Operate (“ATOs”) from OPM with minimal investment in security infrastructure, it did so at the cost of placing the sensitive Confidential Data at a high risk of exposure.

60. USIS likewise ignored the universal recognition by cybersecurity experts that satisfying security compliance criteria is not the same as securing a network. Compliance presents a mere snapshot of how a program meets a specific set of criteria at a given time and, since compliance criteria change slowly, they do not account for day-to-day events in the security landscape that need to be addressed to secure a network.

61. Experts widely agree that proper cybersecurity follows a progression from baseline compliance through world-class cybersecurity controls of the type generally accepted as necessary to protect critical infrastructure such as the Confidential Data entrusted to USIS. The key to achieving effective cybersecurity is to understand an organization’s unique security risk by monitoring and maintaining its systems and controls on an ongoing basis to ensure that the organization continually addresses its evolving security needs.

62. At the time of the Data Breach, USIS’s cybersecurity was at the very low end of this progression due to the Company’s fundamentally flawed compliance-driven approach to security, and, as such, did not begin to address the Company’s true security risk.

D. The Data Breach - USIS’s Substandard Cybersecurity Defenses Leaves the Company Vulnerable to a Cyberattack

63. In the years leading up to the Data Breach there was a dramatic increase in nation-state directed cyberattacks aimed at stealing confidential and sensitive data from government agencies and contractors. In particular, there were myriad warnings about the growing threat of APT attacks.

64. Despite these warnings (which were routinely accompanied by expert and government commentary urging the implementation of defense mechanisms to thwart and/or mitigate such attacks), USIS failed to implement basic and available network defenses to address its security risk.

65. USIS first discovered that it had been hacked on June 5, 2014. While USIS was able to confirm that it had been a victim of a cyberattack, the Company did not immediately know the extent of the attack or whether Confidential Data had been compromised. Accordingly, USIS retained outside legal counsel – Ropes & Gray LLP – and implemented its Computer Incident Response Plan.

66. The computer forensic investigative firm Stroz Friedberg (“Stroz”) was retained to investigate the source and scope of the Data Breach and the extent of loss, if any, of Confidential Data. Stroz was instructed to identify, quarantine, and purge any malware that was installed on USIS’s network by the malicious actors, and to assist in the implementation of new security enhancements designed to minimize any future risks of attack on USIS’s network.

67. Importantly, Stroz was not asked to assess the strength of USIS’s preexisting network security. Rather, in an effort to convince OPM and other government agencies to continue working with USIS, Stroz was asked to focus solely on USIS’s response to, and containment of, the cyberattack.

68. Stroz’s investigation findings are set forth in a “draft” report (the “Stroz Report”) dated October 24, 2014.⁹

⁹ Stroz never provided a final version of the Stroz Report, as OPM terminated its contracts with USIS prior to the completion of the report.

69. Stroz determined that *the breach actually occurred 14 months prior to USIS's initial detection* – on April 19, 2013 – when the malicious actors gained unauthorized access to USIS's network through its Internet-facing SAP Systems managed by Capgemini U.S., LLC (“Capgemini”).¹⁰

70. The malicious actors likely used a well-known and easily preventable SAP security exploit known as the “Invoker Servlet” to break into USIS's SAP Systems. Upon gaining access, the malicious actors installed multiple malware files and password dumping utilities on USIS's SAP Systems without raising any alarms at the Company.

71. Stroz confirmed that on December 31, 2013, *after performing approximately eight months of reconnaissance on USIS's internal systems and defenses without being detected by the Company*, the malicious actors navigated from USIS's SAP Systems to USIS's internal systems where the Confidential Data was maintained.

72. The malicious actors gained access to USIS's internal systems by successfully executing a common “brute force” attack that employed a trial and error hacking technique to guess the correct password for USIS's internal systems.

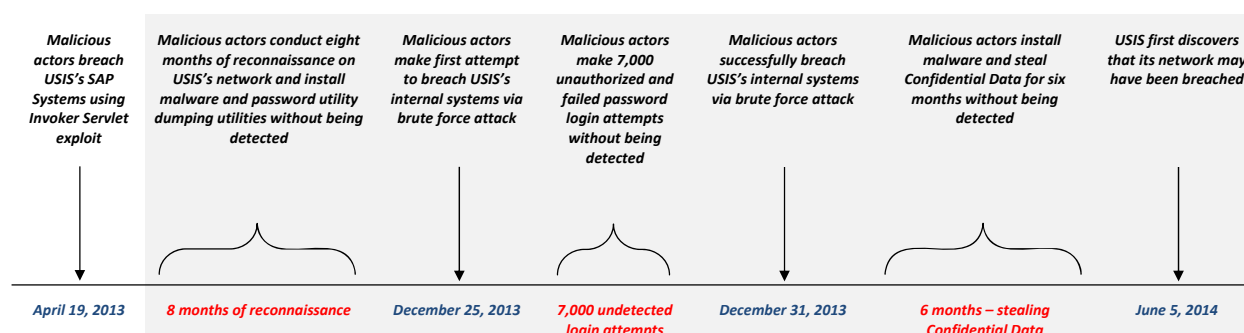
73. Once inside the USIS domain, the malicious actors moved laterally in the USIS environment, harvested data across several USIS systems, and exfiltrated substantial data – including Confidential Data.

74. The last evidence of malicious activity on USIS's network was on July 4, 2014.

¹⁰ Capgemini was hired by USIS to manage and maintain the Company's SAP Systems. Capgemini's responsibilities included partnering with USIS to ensure the security of those SAP Systems.

75. The Stroz Report, which was never fully made public but was reported on, made significant findings, including that the vulnerabilities exploited by the malicious actors to break into USIS's network were well-known and could have been eliminated long before the Data Breach, and that the malicious traffic and activity conducted on USIS's network from April 19, 2013 through June 4, 2014 went undetected for 14 months due to USIS's lack of standard network defenses. These findings tacitly underscore the gross inadequacy of the cybersecurity systems and controls at USIS at the time of the Data Breach.

76. A summary of the Data Breach and the steps taken by the malicious actors that went undetected for 14 months is shown below:



E. USIS's Remediation Efforts Reveal the Fundamental Flaws in USIS's Cybersecurity

77. Following detection of the Data Breach, USIS struggled to preserve its business relationship with OPM through aggressive "all hands on deck" remediation efforts to raise the Company's network security to an acceptable level.

78. However, USIS's remediation efforts only underscored the alarming degree to which the Company was left vulnerable to the Data Breach. The list of critical cybersecurity deficiencies in USIS's network that led to the Data Breach include:

- Failing to properly segment USIS's internal systems containing Confidential Data from USIS's SAP Systems (and from the systems of other Altegrity subsidiaries),

which needlessly exposed USIS's internal systems to malicious activity from the Internet (and from other Altegrity subsidiaries).

- Failing to invest in intrusion detection tools that are necessary to thwart APT attacks, such as deep scanning software like the LIMA and Carbon Black® software used and installed by USIS post-Data Breach.
- Failing to implement basic security defenses to safeguard USIS's internal systems from brute force and other common cyberattacks, including network lockout tools, multi-factor authentication, and a "Kill Switch" to sever USIS's internal systems from the outside world.
- Failing to employ strong password protection to safeguard USIS's internal systems. This is as simple as requiring the entry of a complex, not easily-discovered password to gain access to USIS's internal systems. Here, it took the malicious actors only three days to guess the password needed to gain entry to USIS's internal systems.
- Failing to establish basic internal controls to detect malicious traffic and/or activity on USIS's network. This includes failing to staff USIS with adequate and qualified IT security personnel to monitor USIS's network around the clock, and failing to ensure that IT security personnel were routinely reviewing USIS's network security logs. As a result, USIS missed the evidence of a brute force attack in progress on its network.

F. USIS is Forced to Shutter Its Business and USIS and Altegrity File for Bankruptcy

79. While USIS scrambled to upgrade its cybersecurity measures, OPM conducted a parallel investigation into the Data Breach, during which, OPM insisted that the U.S. Department of Homeland Security's Computer Emergency Readiness Team ("US-CERT") review and analyze USIS's network and network security. US-CERT is a team of government experts under the auspices of the Department of Homeland Security that specializes in responding to major cyberattacks, analyzing threats, and exchanging critical cybersecurity information.

80. Amidst OPM's investigation, on August 6, 2014, news outlets first reported on the Data Breach. News of the Data Breach and the possible exploitation of the Confidential Data were deeply troubling to lawmakers.

81. Rep. Elijah E. Cummings (Md.), a ranking member of the House Oversight Committee, called for an immediate investigation, noting that “[i]t is extremely concerning that the largest private provider of background investigations to the government was hacked.”

82. Sen. Jon Tester (Mont.), a Homeland Security Committee member, echoed Rep. Cummings’ concerns, noting that the Data Breach “is very troubling news” as “Americans’ personal information should always be secure, particularly when our national security is involved. An incident like this is simply unacceptable.”

83. That same day, on August 6, 2014, OPM issued USIS temporary Stop-Work Orders to address the Company’s “IT security issues.” These orders instructed USIS to stop work under the Fieldwork and Support Contracts until OPM could satisfy itself that USIS’s IT risks had been identified and remedied. Given the materiality of the Fieldwork and Support Contracts to USIS, the temporary Stop-Work Orders forced USIS to terminate 2,600 employees (approximately 40% of its workforce).

84. Shortly thereafter, on August 19, 2014, US-CERT concluded that USIS’s network was unsecure and required a complete overhaul. US-CERT highlighted the Company’s lack of proper network segmentation, network monitoring and controls, and security logging, among other issues.

85. US-CERT also recommended an extensive list of basic security recommendations and features for USIS’s new network that should have been in place before the Data Breach such as, firewalls that default to denying access to traffic and permit access only by exception, multi-factor authentication to access to USIS’s network, and intrusion detection and alert tools.

86. US-CERT also instructed USIS to complete an independent security audit. In other words, rather than merely confirming whether USIS’s network security met the minimum

federal security compliance requirements, USIS was to perform a true audit of its information security systems that would account for the Company's specific security needs based on organizational risk.

87. Shortly after the US-CERT Report was issued, on August 22, 2014, OPM notified USIS that because of USIS's insufficient IT security systems and controls, OPM had revoked the Company's ATOs:

[a]s a result of ongoing, extensive work evaluating USIS systems, ***Government experts have concluded that USIS networks were not sufficiently segmented from those of other Altegrity entities to ensure reasonable protection from compromise of USIS-held data or of data held by other Altegrity entities.*** The Government has determined that ***the full extent of the compromise of the Altegrity entities may never be known due to a lack of complete security logs and standard cybersecurity equipment that could have provided this information.*** As a result, the Government considers all data housed on the networks of the Altegrity entities to have been exposed." (emphasis added).

88. In light of the extensive security enhancements that USIS needed to implement to achieve "***a reasonably secure network that is resilient against intrusion,***" OPM required USIS to obtain new security authorizations and accreditation before it could resume performing background investigation work for OPM. (emphasis added).

89. Other federal agencies, including the Department of Homeland Security, sent similar notifications to USIS on or around the same time. The impact of this business interruption was devastating to USIS, and the Company's post mortem remediation efforts were simply too little too late to salvage USIS's background investigation business.

90. On September 9, 2014, OPM notified USIS that it would not renew USIS's Fieldwork and Support Contracts that were due to expire on September 30, 2014.

91. The following day, OPM further informed USIS that OPM awarded a new fieldwork contract to KeyPoint among others, and that it awarded a new support services contract to NTConcepts.

92. The loss of these contracts not only meant the loss of the most critical revenue stream for USIS and Altegrity – approximately \$3 billion – but it also carried substantial collateral costs for USIS as the Company was required to transition all of the work under the contracts to its competitors and shift its focus to winding down its business and preparing additional submissions to OPM.

93. USIS was also the subject of a congressional investigation, heightened government scrutiny, and negative publicity that destroyed its reputation and future prospects.

94. The foregoing caused USIS along with its parent company, Altegrity, to file voluntary petitions for relief under Chapter 11 of the United States Code in the United States Bankruptcy Court for the District of Delaware on February 8, 2015. The Plan was filed on March 30, 2015 and confirmed by the Bankruptcy Court on August 14, 2015.

G. USIS is Subjected to Congressional Scrutiny

95. Congressional scrutiny of USIS continued even after the Company lost its federal contracts. According to Rep. Elijah Cummings, the House Oversight Committee received a briefing from security experts at the Department of Homeland Security, OPM, and the Office of the Director of National Intelligence, which revealed that “*USIS data security measures appear to be inferior to those of the government.*” Moreover, according to Rep. Cummings, USIS and Altegrity were not complying with the Committee’s requests for information to investigate, *inter alia*, the Company’s security posture.

96. The House Oversight Committee conducted a hearing on cybersecurity on April 22, 2015. During the hearing, Rep. Cummings, referring to USIS’s lack of internal controls, was critical of USIS’s apparent practice of cutting corners on security to boost profits:

USIS is currently at the center of a billion dollar civil fraud suit brought by the Justice Department for allegedly ‘dumping’ incomplete background investigation reports to OPM over a 4 ½ year time period. According to the Justice

Department, USIS deliberately took this action to increase its revenues and profits [posing a serious threat to national security]. *Apparently, the company's desire to increase profits also may have been to blame for its failure to make the cyber investments necessary to secure the large amounts of sensitive personal information it should have been protecting on its networks.*

H. Defendant Rowlands and the Board Had a Duty to Oversee and Monitor USIS's Response to Known Cybersecurity Risks

97. Defendant Rowlands and the Board had a fiduciary obligation to oversee and monitor USIS's response to the known risk of a cyberattack. Cybercrime is a risk management issue that is well-understood to be an enterprise-risk issue requiring board oversight.

98. Lloyd's of London's Risk Index 2013 reported that cybersecurity was the second-highest perceived risk for business leaders in the U.S. and Canada.

99. SEC Commissioner Luis Aguilar emphasized the need for board oversight over companies' cybersecurity measures in a June 2014 speech entitled "*Cyber Risks in the Boardroom*," stating that:

[E]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and [the] lasting reputational harm [that could result from a cyberattack], there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber threats. (emphasis added).

100. Similarly, in an article entitled "*Cyber Security is a Board-Level Issue*" published by American International Group, Inc. ("AIG"), AIG stressed that while day-to-day responsibility for cybersecurity may lie with senior management and IT personnel, the rapid escalation in cyberattack threats "*prompted the evolution of cyber risk from being primarily an*

IT threat to an enterprise wide management issue needing board-level attention.” (emphasis added).¹¹

101. Further, in addition to cybersecurity being an enterprise risk issue requiring Defendant Rowlands’ and the Board’s oversight, Defendant Rowlands and the Board had an increased duty to oversee and monitor USIS’s response to the known risk of an attack due to: (1) the materiality of USIS’s government contracts to the Company’s operations; (2) the consequences of a cyberattack and the importance of safeguarding the Confidential Data on USIS’s network; (3) the dramatic increase in cyberattacks on government contractors in the years leading up to the attack; and (4) the known lack of internal controls at USIS.

1) The OPM Contracts Were Material to USIS’s Operations

102. USIS was the business segment that generated the most revenue for Altegrity. The Company performed background investigations, information management, and security services to various federal agencies, including OPM.

103. USIS’s five-year Support Contract with OPM was valued at approximately \$288 million. USIS’s five-year Fieldwork Contract was valued at approximately \$2.46 billion, making it the largest contract held by USIS, and a major revenue driver for both USIS and Altegrity.

104. Prior to the Data Breach, USIS employed over 5,700 individuals and generated approximately \$537.3 million in revenue for the twelve months ended June 30, 2014. USIS’s revenue accounted for 39% of Altegrity’s consolidated revenue during the same timeframe.

¹¹ See “*Cyber Security is a Board-Level Issue*” July 2016 available at: <https://www.aig.com/knowledge-and-insights/k-and-i-article-cyber-security-board-level-issue>.

2) Safeguarding the Confidential Data Was Critical to USIS's Relationship with OPM and to National Security

105. Defendant Rowlands and the Board knew that safeguarding the Confidential Data USIS collected and maintained on its computer network was critical to national security and to USIS's relationship with OPM.

106. Pursuant to its contracts with OPM, USIS was responsible for conducting the investigatory fieldwork on individuals seeking new or continued employment with federal agencies or one of their contractors.

107. The information USIS collected included extremely personal and potentially damaging information about the applicant. In addition to conducting interviews and performing background checks on applicants, including education, employment, criminal history, legal, and credit checks, USIS also gathered information concerning whether an applicant engaged in extramarital affairs, past drug use, had gambling problems, required psychological treatment or counseling, etc.

108. Because this Confidential Data could be used to identify and exploit federal employees to compromise U.S. missions, it was a treasure chest for malicious actors and other enemies of the state. Safeguarding the Confidential Data USIS collected and maintained on its computer network was critical to national security and to maintaining USIS's business relationship with OPM.

3) The Nature of USIS's Business Made it Target for an APT Attack

109. Defendant Rowlands and the Board knew that USIS was at risk of an APT attack due to the nature of the Company's business and its possession of Confidential Data that could be used to compromise federal employees entrusted with the nation's most top-secret information.

110. Indeed, in the years leading up to the Data Breach, there were frequent warnings about the growing threat of nation-state directed APT attacks on the government and government contractors such as USIS. The increased threat of APT attacks had been widely publicized by the media and the government due to the high profile targets victimized by the attacks, and the sensitivity of the data stolen during the attacks. Some of the most infamous of these APT attacks included:

- the 2003 “Titan Rain” attack perpetrated by China against NASA and the FBI, among other U.S. Government agencies, to gain military data;
- the 2006 “Sykipot Attacks” aimed primarily at U.S. and U.K. organizations including defense contractors, telecommunications companies, and government departments;
- the 2008 “Buckshot Yankee” attack on the U.S. Department of Defense, which was considered the “worst breach of U.S. military computers in history”;
- the 2009 “GhostNet” attack perpetrated by China that compromised computers in over 100 countries, and infiltrated network devices associated with embassies and government ministries;
- the “July 2009 DDoS Attack” to target commercial and government websites in the U.S. and in South Korea via “brute force” tactics;
- the 2010 “Stuxnet Worm” attack against Iran, targeting systems containing data concerning Iranian industrial infrastructure and nuclear facilities;
- the 2010 “Operation Aurora” attack waged by China on Google and other major organizational enterprises in the U.S. aimed at gaining access to and potentially modifying source code repositories at high tech, security, and defense contractors;
- the 2011 “RSA SecureID Attack” directed at security company RSA to steal information related to RSA’s SecurID two-factor security authentication products;
- the 2012 attack aimed at stealing PII that was perpetrated against Global Payments, a company that helped Visa and MasterCard process transactions for merchants; and
- the 2013 attack by China on *The New York Times* to gain access to the passwords of reporters and other employees.

111. U.S. Government officials likewise issued numerous public warnings to take proper precaution to defend against APT attacks.

112. For example, on February 29, 2012, during a public hearing before the U.S. House of Representatives, NASA Inspector General Paul Martin testified about the growing concern over APT attacks. Specifically, General Martin testified that in 2011 alone, NASA was the victim of 47 APT attacks, 13 of which successfully compromised NASA computers. In one such attack, malicious actors stole user credentials for more than 150 NASA employees, which could have been used to gain unauthorized access to NASA systems.

113. Days later, on March 1, 2012, following a speech at the McConnell Center at the University of Louisville, U.S. Defense Secretary Leon Panetta revealed that “a major cyber attack” is what keeps him up at night, and cautioned that government agencies, government contractors, and companies all need to take special care to defend against such attacks:

We are literally getting hundreds or thousands of attacks every day that try to exploit information in various [U.S.] agencies or departments. . . . There are, obviously, growing technology and growing expertise in the use of cyber warfare,” and “[t]he danger is, I think, the capabilities are available in cyber to virtually cripple this nation: to bring down the power grid, to impact on our governmental systems, to impact on Wall Street and our financial system and to literally paralyze this country. (emphasis added)

114. Defendant Rowlands herself warned of the growing threat of cyberattacks and cautioned companies like USIS to take a proactive approach to cybersecurity, including by employing adequate and qualified IT security personnel to identify and fix network vulnerabilities and to continually test and improve network security to address new risks.

115. In a March 21, 2012 interview with *WashingtonExec*, Defendant Rowlands acknowledged the growing threat of cyberattacks on organizations like USIS and the need to be proactive to defend against such attacks. During that interview, Defendant Rowlands stated that “compliance and cybersecurity” were two of “the most significant issues for business today” and

emphasized that companies handling confidential information like USIS had to be proactive with respect to preventing cyberattacks:

I think another huge issue, and you read more and more about this, is clearly in the area of cyber security. ***There are multiple threats facing companies today, and companies must be proactive to prepare for and defend against cyber attacks. IT infrastructure protection is extremely critical, particularly for companies that handle confidential information and maintain customer information on their computer systems. Companies can, and should, take precautions and not wait for a problem to occur.*** (emphasis added)¹²

116. Defendant Rowlands further emphasized the need for companies to have policies in place to routinely test their cybersecurity safeguards:

You can't afford to wait for something to happen. ***You have to have policies and training in place, have smart people working your IT areas and you have to do your own intrusion testing – and conduct in a very realistic way.*** I always tell our IT security people to focus on finding where the gaps are and, if they find a gap, don't take that as a failure. It means we found it and that's good because then we can take remedial actions. I really think it's about being prepared, having the best talent available on your IT and related teams ***and making sure you're constantly testing your system and procedures.*** (emphasis added)¹³

117. Accordingly, Defendant Rowlands and the Board knew of the cybersecurity risks USIS was facing and the importance of preventing and/or thwarting such an attack. In light of these known risks, Defendant Rowlands and the Board had a duty, through their oversight role, to ensure that USIS senior management was taking the necessary steps to address the known risk of a cyberattack:

Directors are required to satisfy themselves, through their risk oversight role, that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are

¹² The full interview with Defendant Rowlands can be found at: <http://www.washingtonexec.com/2012/03/altegrity-ceo-sharon-rowlands-talks-mobile-and-cybersecurity-you-cant-afford-to-wait-for-something-to-happen/#.WDThbIrKUK>.

¹³ *Id.*

functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization.

The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risk that underlie its risk oversight. (emphasis added).¹⁴

118. Nevertheless, despite knowing of the risk of a cyberattack on USIS and the Board's obligation to oversee USIS's response to the risk, Defendant Rowlands and the Board utterly failed to monitor or oversee USIS's cybersecurity practices, thus disabling themselves from being informed of what steps, if any, USIS was taking to address the risk.

4) Defendant Rowlands Knew USIS Suffered from Weak Internal Controls

119. In addition to knowing of the increasing risk of a cyberattack that could (and did) materially impact USIS, Defendant Rowlands and the Board knew that USIS suffered from weak internal controls that necessitated the Board's careful oversight and monitoring. Specifically, USIS senior management had a history of taking shortcuts and engaging in fraudulent activities in order to increase revenues and earn bonuses.

120. Since August 2011, USIS was answering to Congress and the Department of Justice ("DOJ") over allegations that USIS was fraudulently reporting to OPM that background investigations had been completed, when in fact they had not – a practice referred to as "dumping." Defendant Rowlands and the Board were aware of the allegations, as USIS received and responded to a subpoena for records in January 2012.

¹⁴ Harvard Law School Forum on Corporate Governance and Financial Regulation, "*Risk Management and the Board of Directors – An Update for 2012*" posted January 3, 2012, available at: <https://corpgov.law.harvard.edu/2012/01/03/risk-management-and-the-board-of-directors-an-update-for-2012/>.

121. As a result of a whistleblower claim filed by a former USIS executive, the Office of Inspector General (“OIG”) of OPM began investigating USIS in late 2011. The DOJ subsequently intervened and filed a complaint against USIS, captioned *United States of America ex rel. Blake Percival v. U.S. Investigations Services*, Civil Action No. 11-CV-527-WKW.

122. The DOJ alleged that beginning in March 2008 and continuing at least through September 2012, “USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company’s revenues and profits.” On August 19, 2015, the DOJ announced that USIS agreed to settle the whistleblower action for \$30 million.

123. During a hearing before the Committee on Oversight and Government Reform concerning the scandal, Rep. Carolyn Maloney (N.Y.) heavily criticized USIS’s lack of regard for the national security implications of its fraudulent actions: “[t]hey’ve created a national-security threat and I would call that very serious.”

124. As information relating to USIS’s dumping practices came to light, Congress and various government agencies began to scrutinize the quality and integrity of USIS’s background investigation work. For example, USIS was criticized for its performance of the 2011 background investigation of former intelligence contractor Edward Snowden, who infamously leaked classified information from the National Security Agency, revealing numerous global surveillance programs.

125. On February 7, 2014, *The Wall Street Journal* published an assessment of USIS’s background investigation on Mr. Snowden by the Office of the Director of National Intelligence, highlighting a number of significant issues in USIS’s investigation process, including the failure to check certain of Mr. Snowden’s references, the failure to verify Mr. Snowden’s past

employment with the Central Intelligence Agency, and the failure to do an independent check of an unspecified security violation in Mr. Snowden's file.

126. USIS was likewise criticized for its performance of the 2007 background check on former defense contractor Aaron Alexis who notoriously used his security clearance to bring a gun to the Washington Navy Yard and kill twelve people.

127. Senator Claire McCaskill heavily criticized USIS for taking shortcuts with the national security:

From Edward Snowden to Aaron Alexis, what's emerging is a pattern of failure on the part of this company, and a failure of this entire system, that risks nothing less than our national security and the lives of Americans. (emphasis added).

128. At a February 11, 2014 hearing, Ranking Member Rep. Elijah Cummings noted that the DOJ's fraud allegations against USIS had raised serious allegations regarding USIS and its management:

In 2007, USIS was purchased by a private equity firm known as Providence Equity Partners. The Committee's investigation revealed that directly after this acquisition, USIS adopted aggressive new financial incentives to accelerate its work. During this period, USIS executives received huge bonuses, including more than \$1 million for the company's CEO, Bill Mixon, and about \$470,000 for the company's Chief Financial Officer. The Justice Department alleges that both officials were 'fully aware of and, in fact, directed the dumping practices.' USIS also received millions of dollars in bonus payments from OPM for its seemingly incredible progress, including \$2.4 million in 2008, \$3.5 million in 2009, and \$5.8 million in 2010.

In the wake of this scandal, the company's CEO, CFO, and nearly two dozen other officials have resigned, been terminated, or left the company. In fact, just yesterday, USIS informed us that the President of its Investigations Services Division [Mr. Johnny Tharp] has also now resigned. (emphasis added).

129. The lack of internal controls at USIS and the Company's history of cutting corners to increase revenues should have raised a red flag to Defendant Rowlands and the Board that USIS required careful oversight and monitoring and should not be left to its own devices

with respect to known enterprise-risks (such as cybersecurity risks) that could impact national security, as well as the Company's relationship with OPM.

130. Defendant Rowlands' failure to oversee USIS's cybersecurity practices in light of the known cybersecurity risks and the lack of internal controls at USIS was a breach of her duty of loyalty and good faith.

I. In the Face of the Known Risks, Defendant Rowlands and the Board Consciously Failed to Monitor and Oversee USIS's Cybersecurity Practices

131. Despite knowing that there was an increased risk of a cyberattack on USIS as a government contractor and custodian of Confidential Data and USIS's lack of internal controls, Defendant Rowlands and the Board breached their fiduciary duties by consciously failing to monitor and oversee USIS's cybersecurity practices in the face of such risks.

132. Based on a review of the Joint Board minutes from February 12, 2012 to March 31, 2014, Defendant Rowlands and the Board failed to oversee or monitor USIS's cybersecurity safeguards and practices in face of the known risk of an attack. The Board Minutes reflect that no information concerning USIS's cybersecurity practices was reported to the Board during these meetings, nor did the Board delegate its direct oversight responsibility relating to USIS's security measures in the face of such risks to any Board committee.

133. For example, according to the Board Minutes, no one from USIS reported to the Board on the status of USIS's cybersecurity procedures and practices. Defendant Rowlands and the Board were not briefed about the cybersecurity environment, vulnerabilities, threats, or what steps USIS was taking to meet any such threats. Similarly, there was no discussion as to USIS's structure, operation, and testing of security programs, the Company's budget for upgrading or maintaining cybersecurity protocols, trends in the industry or any emerging issues relating to cybersecurity.

134. Rather, the Board Minutes indicate that USIS was primarily focused on driving growth, increasing productivity, and reducing costs. For example, at the December 12, 2012 Board meeting (four months prior to the Data Breach), Defendant Rowlands provided a status report on USIS and its ISD business (USIS's former CEO Peter Masanotti had stepped down due to fraud allegations) that focused primarily on the hiring of new investigators and the challenges involved with training new employees.

135. Similarly, USIS's report to the Board in February 2013 (just two months prior to the Data Breach) highlighted that the primary focus over the next 90 days would be on operation execution and the quality of service delivery.

136. During the May 9, 2013 Board meeting – one month after the malicious actors breached USIS's systems – USIS's CEO merely reported, among other things, that USIS was under pricing pressure from the U.S. government and reported on the importance of diversification in an effort to increase shareholder value.

137. Neither Defendant Rowlands nor any other Board member questioned USIS about its cybersecurity practices and procedures, the increasing threat of a cybersecurity attack on USIS, or whether additional safeguards were or should be implemented.

138. Instead, Defendant Rowlands and the Board left it to USIS to address the increasing risk of a cyberattack without any monitoring or oversight by the Board. This oversight failure resulted in Defendant Rowlands and the Board being completely disabled from being informed of the risks requiring their attention.

139. Defendant Rowlands' failure to oversee USIS's cybersecurity practices in light of the known cybersecurity risks and the lack of internal controls at USIS was a breach of her duty of loyalty and good faith.

FIRST CAUSE OF ACTION**Against Defendant Rowlands
for Breach of Fiduciary Duty**

140. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

141. By reason of her position as a director and/or fiduciary of USIS, and because of her ability to control the business and corporate affairs of USIS, Defendant Rowlands owed USIS fiduciary obligations of loyalty and due care, and was required to use her utmost ability to control and manage USIS in a fair, just, honest, and equitable manner.

142. Defendant Rowlands knew through direct knowledge that (1) there were increasing cybersecurity threats aimed at USIS as a government contractor which presented a substantial and material risk to USIS; (2) such cyber threats were increasing in frequency and sophistication; and (3) that USIS suffered from weak internal controls that necessitated careful oversight and monitoring by the Board.

143. As described herein, Defendant Rowlands knowingly violated her fiduciary duties by failing to exercise her oversight duties with respect to USIS's cybersecurity measures, thus completely disabling herself from being informed as to what steps, if any, USIS management was taking to address the known risk of a cyberattack.

144. As a direct and proximate result of Defendant Rowlands' breaches of her fiduciary obligations, USIS was significantly damaged, as USIS: (1) suffered the devastating Data Breach that resulted in the exfiltration of the Confidential Data of tens of thousands of federal employees and applicants seeking sensitive national security clearances; (2) received Stop-Work Orders from OPM; (3) was forced to terminate its workforce and spend millions of dollars to remediate its network; (4) lost its lucrative contracts with OPM and other federal

agencies; (5) ceased to exist as a going concern; and (6) was exposed to litigation from federal agencies and federal employees whose data was compromised. Defendant Rowlands' breaches of her fiduciary duties also caused USIS and its parent company Altegrity to file for Chapter 11 bankruptcy and threatened the wholesale degradation of national security.

145. As alleged herein, Defendant Rowlands is liable for her misconduct.

146. Plaintiff, on behalf of the Committee and USIS, has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment and relief in its favor against the Defendant, as follows:

- A. Awarding Plaintiff the amount of damages sustained by USIS as result of the Defendant's breaches of fiduciary duties;
- B. Awarding Plaintiff the costs and disbursements of the action, including reasonable attorneys' fees and experts' fees, costs and expenses; and
- C. Granting such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Dated: May 26, 2017

BERNSTEIN LIEBHARD LLP

/s/
Stanley D. Bernstein (bernstein@bernlieb.com)
Stephanie M. Beige (beige@bernlieb.com)
Laurence J. Hasson (hasson@bernlieb.com)
10 East 40th Street
New York, NY 10016
Telephone: (212) 779-1414
Facsimile: (212) 779-3218

*Attorneys for Plaintiff and The Specified Claims
Oversight Committee*

(00408417-2)